ATTORNEY DOCKET NO.: 50P4257.05

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION ENTITLED:

WIRELESS MODULE SECURITY SYSTEM AND METHOD

By:

Akihiko Toyoshima

CERTIFICATE OF EXPRESS MAILING

"Express Mail" Label: EL645989657 US

Date of Deposit: October 5, 2001

I hereby certify that the above-referenced application papers are being deposited with the United States Postal Service "Express-Mail-Post-Office-to-Addressee" service under 37 C.F.R. §1.10 on the date indicated above and is addressed to the Commissioner for Patents, Washington, D.C. 20231.

Carrie Merzbacher

WIRELESS MODULE SECURITY SYSTEM AND METHOD

This application incorporates herein by reference U.S. Patent Application Serial Number 09/_____, of Akihiko Toyoshima, for SYSTEM AND METHOD FOR ACTIVATION OF A WIRELESS MODULE, filed concurrent herewith (Sony IPD 50R4257.01); U.S. Patent Application Serial No. 09/_____, of Akhiko Toyoshima, for HOME NETWORK USING WIRELESS MODULE, filed _____, 2001 (Sony IPD 50P4257.02); U.S. Patent Application Serial No. 09/_____, of Akhiko Toyoshima, for MULTIPLE WIRELESS FORMAT PHONE SYSTEM AND METHOD, filed concurrent herewith (Sony IPD No. 50P4257.03); U.S. Patent Application Serial No. 09/_____, of Akhiko Toyoshima, for WIRELESS MODEM MODULE SERVER SYSTEM, filed _____, 2001 (Sony IPD No. 50P4257.04); U.S. Patent Application Serial No. 09/ _____, of Akihiko Toyoshima, for A DEFAULT PORTAL SITE ACCESS WITH WIRELESS MODULE, filed _____, 2001 (Sony IPD 50R4257.06); and U.S. Patent Application Serial No. 09/ _____, of Akihiko Toyoshima, for SYSTEM, METHOD AND APPARATUS FOR EBEDDED FIRMWARE CODE UPDATE, filed concurrent herewith (Sony IPD 50R4257.07); and U.S. Patent Application Serial Number 09/928,582, of Baranowski, et al.; for WIRELESS MODULE, filed August 13, 2001 (Sony IPD 50N3390); and Provisional Patent Application Serial No. 60/240,001; of Juan, et al, for PORTABLE WIRELESS MODEM, filed October 13, 2000 (Sony IPD 50P4257), the benefit whose priority date is hereby claimed.

Copyright Notice

Field of the Invention

This invention relates generally to the field of removable data storage devices. More particularly, this invention relates to a security system and method for a data storage and wireless transmission module.

Background of the Invention

The need for portability of data has increased over the years, and has spurred the development of removable memory devices. For example, Memory Stick™ is a removable data storage device made by Sony Corporation and is a recordable integrated circuit (IC) digital storage device having a storage capacity greater than a standard 3.5 inch floppy disk. Most importantly, Memory Stick™ is smaller than a stick of gum, very lightweight, and therefore ultra-portable. However, the need for accessability to people, information, and data has also increased and spurred the creation of an ultra-portable accessability device.

A wireless module which provides accessability and portability to peripheral devices without increasing their cost or exceeding their related space limitations is so provided in a co-pending Patent Application Serial Number _____, (Sony IPD 50R4257.01) entitled SYSTEM AND METHOD FOR ACTIVATION OF A WIRELESS MODULE; and U.S. Patent Application Serial Number 09/928,582, of Baranowski, et al.; for WIRELESS MODULE, filed August 13, 2001 (Sony IPD 50N3390). In these co-pending patent applications, the wireless module described can be shared with any type of peripheral device which supports such an interface. If the wireless module described is lost or stolen, it could be easily used for illegal purposes and for the perpetration of any crime.

Summary of the Invention

In view of the foregoing, a security system for a wireless module is provided to prevent the unauthorized and illegal use of the wireless module.

In particular, the wireless module, in one embodiment is provided with security data. In one embodiment, the security data is stored to the wireless module and is provided to the user of the wireless module during initialization and establishment of a wireless module account with an activation center. In another embodiment, the security data is provided to any number of peripheral devices which utilize the removable wireless module. In a further embodiment, the security data along with a complete electronic serial number (ESN) is provided to any number of peripheral devices which utilize the wireless module for a further security measure. In yet another embodiment, the wireless module obtains and stores peripheral device data from the peripheral devices which are provided with the security data.

These and other features and advantages of the invention will be understood upon the consideration of the following detailed description of the invention and accompanying drawings. The features of the invention believed to be novel are set forth with particularity in the appended claims. The invention itself however, both as to organization and method of operation, together with further objects and advantages thereof, may be best understood by reference to the following description taken in conjunction with the accompanying drawing.

Brief Description of the Drawing

The following detailed description, given by way of example, and not intended to limit the present invention solely thereto, will best be understood in conjunction with the accompanying drawings in which:

FIGURE 1 is a block diagram of one embodiment of a wireless module.

FIGURE 2 is a flow diagram illustrating the steps of one embodiment of a method for providing security to the wireless module.

FIGURE 3 is a flow diagram illustrating the steps of one embodiment of a method for providing security to the wireless module by matching security data.

FIGURE 4 is a flow diagram illustrating the steps of another embodiment of a method for providing security to the wireless module by matching some combination of security data.

Detailed Description of the Invention

While the present invention has been particularly shown and described with reference to an embodiment(s), it will be understood that various changes and modifications may be made without departing from the spirit and scope of this invention. It is intended that the appended claims be interpreted to cover the embodiments described herein and all equivalents thereto.

FIGURE 1 depicts one embodiment of a wireless module 100 which includes an antenna 10 connected to a transceiver circuit 20. Transceiver circuit 20 includes a duplexer 30, a transmitter 40, and a receiver 50. Transmitter 40 and receiver 50 of transceiver circuit 20 are connected to a baseband signal processor circuit 60. Baseband signal processor circuit 60 is connected to a microprocessor 70. Memories 80 and an interface input/output (I/O) 90 are also connected to microprocessor 70. A host or peripheral unit/device 150 is connected to wireless module 200 through interface I/O 90.

In operation, wireless module 100 receives a signal(s) containing data packets through antenna 10 and forwards the received signals and data packets to duplexer 30, through receiver 50, and to baseband signal processor circuit 60. The data packets/received signals will then be forwarded to microprocessor 70 and through interface I/O 90 to peripheral device/host 150. For example, host/peripheral device 150 may be a PC, laptop, PDA, wireless telephone, or any other type of device or unit which can handle the data packets/received signals. Wireless module 100 receives and transmits data packets/received signals utilizing at least one wireless format selected from the group consisting of CDMA ONE, CDMA 2000 1X, CDMA 2000 3X, CDMA 1X EV, Wideband CDMA, GSM, GPRS and EDGE. In case peripheral

device/host 150 engages in simultaneous transmission and reception of data packets, duplexer 30 and memories 80 are utilized.

FIGURE 2 shows a flow diagram 200 illustrating the steps of one embodiment of a method for providing security to wireless module 100 (shown in FIGURE 1). The first step of the method for providing security to wireless module 100 includes an activation process 210 after which security data (not shown) is provided to wireless module 100. In one embodiment, the security data includes a security code (not shown). Step 220 illustrates the issuing of the security code after wireless module 100 has been activated. Flow diagram 200 further illustrates the encrypting of the security code in step 230 prior to issuing the security code through wireless transmission to wireless module 100 and decrypting the security code in step 240 prior to storing the security code.

Step 250 illustrates one embodiment of the method for providing security to wireless module 100 by storing the security code inside wireless module 100. Flow diagram 200 illustrates the conclusion to one embodiment of the method for providing security to wireless module 100 by step 260 where the security code is notified to a user (not shown). In another embodiment, the method for providing security to wireless module 100 provides that the security code is also stored inside/to a peripheral device (not shown). When the security code is also stored inside the peripheral device, step 260 may be eliminated.

FIGURE 3 shows a flow diagram 300 illustrating the steps of one embodiment of a method for providing security to wireless module 100 (shown in FIGURE 1) by matching security data. Once the user of the peripheral device is notified of the security code, step 310 requires the user to input the security code into the peripheral device in order to have authorized access for the utilization of wireless module 100. If the security code input by the user into the peripheral device matches the security code stored in wireless module 100 then step 320 illustrates that authorized access for the utilization of wireless module 100 is granted. If the security code input by the user into the peripheral device does not match the security code stored in wireless module 100 then step 330 illustrates that the process for authorized

access for the utilization of wireless module 100 fails and access is not granted. In another embodiment, the security code is also stored inside the peripheral device so that once the wireless module 100 is in electronic data communication with the peripheral device the separately stored security codes may be automatically compared and the user's input not required, as a further option.

FIGURE 4 shows a flow diagram 400 illustrating the steps of another embodiment of a method for providing security to wireless module 100 (shown in FIGURE 1) by matching some combination of security data. In another embodiment, wireless module 100 is provided with a complete electronic serial number (not shown) which is stored inside the peripheral device as a security measure. Once the user of the peripheral device is notified of the security code, step 410 requires the user to input the security code into the peripheral device in order to have authorized access for the utilization of wireless module 100. If the security code input by the user into the peripheral device matches the security code stored in wireless module 100 then step 420 illustrates that a further security combination process is performed. If the electronic serial number stored in the peripheral device matches the electronic serial number of wireless module 100 then step 430 illustrates that the process for authorized access for the utilization of wireless module 100 is granted. However, if the security code input by the user into the peripheral device does not match the security code stored in wireless module 100 then step 440 illustrates that the process for authorized access for the utilization of wireless module 100 fails and no further step is taken.

Flow diagram 400 illustrates the conclusion to another embodiment of the method for providing security to wireless module 100 by step 450 where the electronic serial number stored in the peripheral device does not match the electronic serial number of wireless module 100, then the process for authorized access for the utilization of wireless module 100 fails and access is not granted. In a further embodiment, the method for providing security to wireless module 100 by matching some combination of security data provides the peripheral device with peripheral device data (not shown) and stores the peripheral device data to wireless module 100.

When the peripheral device data is also stored inside wireless module 100, step 420 may be further extended such that once the electronic serial number stored in the peripheral device matches the electronic serial number of wireless module 100 and the peripheral device data stored in wireless module 100 matches the peripheral device data of the peripheral device, then step 430 illustrates that the process for authorized access for the utilization of wireless module 100 is granted.

In yet another embodiment, the security code is also stored inside the peripheral device so that once the wireless module 100 is in electronic data communication with the peripheral device the separately stored security codes may be automatically compared and the user's input not required which eliminates step 410 and triggers automatic security combination process as illustrated by step 420, as a further option which may be specified by the user.

In order to provide security to wireless module 100, a wireless module activation server (not shown) includes at least one user activation web site (not shown) utilized to transmit security data during the activation process (not shown). The wireless module activation server may also be utilized to automatically and/or remotely activate and deactivate wireless module 100 in the event of a loss, theft, or a failure of any one of the methods for providing security to wireless module 100. The user activation web site is in electronic data communication with wireless module 100 and the peripheral device, and may also store the security data in connection to a wireless module account (not shown).

Wireless module 100 may store any embodiment of the security data to any number of user authorized peripheral devices.

Thus it is apparent that in accordance with the present invention, an apparatus that fully satisfies the objectives, aims and advantages is set forth above. While the invention has been described in conjunction with specific embodiments, it is evident that many alternatives, modifications, permutations and variations will become apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended that the present invention embrace all such alternatives, modifications and variations as fall within the scope of the appended claims.